Claims

WHAT IS CLAIMED IS:

1. A method for generating temporarily assigned identity information, comprising:

authenticating identity information associated with a request received from a requestor for accessing a service;

generating temporarily assigned identity information for the requestor;

updating a protected identity directory with the temporarily assigned identity information; and

transmitting the request and the temporarily assigned identity information to the service on behalf of the requestor, wherein the service accesses the protected identity directory with the temporarily assigned identity information to authenticate the requestor for access.

2. The method of claim 1 further comprising:

generating a mapping between the identity information and the temporarily assigned identity information; and

storing the mapping in a local identity mapping store.

3. The method of claim 2 further comprising, synchronizing the local identity mapping store and the mapping with one or more addition local identity mapping stores.

4. The method of claim 1 wherein the generating further includes assembling an aggregate identity configuration for the requestor from one or more authoritative identity stores before generating the temporarily assigned identity information.

5. The method of claim 1 further comprising, removing the temporarily assigned identity information from the protected identity directory after detecting a

terminating event that terminates the authenticity of the temporarily assigned identity information.

6. The method of claim 5 further comprising recycling a storage space occupied by the temporarily assigned identity information for use in a subsequent iteration of the method.

7. The method of claim 1 further comprising:

detecting dynamic changes made on at least a portion of the identity information, wherein the changes are detected within the protected identity directory; and

synchronizing the temporarily assigned identity information with the changes.

8. The method of claim 1 further comprising:

detecting dynamic changes made on at least a portion of the identity information, wherein the changes are detected within the protected identity directory; and

synchronizing the changes with one or more authoritative identity stores impacted by the changes.

9. The method of claim 1 further comprising:

detecting changes made on at least a portion of the identity information, wherein the changes are detected within the protected identity directory; and

logging the changes for subsequent update with one or more authoritative identity stores impacted by the changes.

10. A method for generating temporarily assigned identity information, comprising:

acquiring a request for a service;

authenticating the request;

compiling an identity configuration for the request;

generating temporarily assigned identity information for the request using the identity configuration; and

transmitting the temporarily assigned identity information and the request to the service.

11. The method of claim 10 wherein the intercepting further includes, intercepting the request, where the request originates from a requestor's service over an insecure network.

12. The method of claim 10 wherein the transmitting further includes, transmitting the temporarily assigned identity information and the request to the service within a secure network.

13. The method of claim 10 further comprising accessing, by the service, a protected identity directory to authenticate the request using the temporarily assigned identity information.

14. The method of claim 10 further comprising:

acquiring an additional request issued from a same-requestor that is associated with the request, wherein the additional request is for an additional service;

authenticating the additional request; and

transmitting the temporarily assigned identity information and the additional request to the additional service.

15. The method of claim 10 further comprising, forcing the temporarily assigned identity information to expire upon detection of a terminating event.

16. The method of claim 10 wherein the compiling further includes aggregating identity policies from one or more authoritative identity stores, wherein the identity

policies are associated with a requestor that issued the request for the service.

17. An identity information management system, comprising:

a proxy server that intercepts requests made for services, wherein the requests are associated with requestors;

a local identity mapping store for housing mappings between temporarily assigned identity information and identity configurations, the temporarily assigned identity information and the identity configurations are generated from identity information provided with the requests; and

a protected identity directory updated with the temporarily assigned identity information and accessed by the services in order to authenticate the requests, wherein the requests and the temporarily assigned identity information are transmitted to the services on behalf of the requestors.

18. The identity information management system of claim 17 further comprising a local identity mapping store synchronizer that synchronizes the mappings in the local identity mapping store with one or more additional local identity mapping stores.

19. The identity information management system of claim 17 wherein the local identity mapping store, the protected identity mapping store, and the services are accessible from a secure network.

20. The identity information management system of claim 17 wherein the identity configurations are generated from one or more authoritative data stores associated with the requestors.

21. The identity information management system of claim 17, wherein the identity information includes at least one of an identification, a password, a certificate, a token, a biometric value, a hardware value, a network connection value, and a time value.

22. The identity information management system of claim 17, the temporarily assigned identity information is monitored and removed them from the protected identity directory and the local identity mapping store when terminating events are detected.

23. The identity information management system of claim 17, wherein the temporarily assigned identity information is randomly or deterministically generated.

24. The identity information management system of claim 17, a storage space associated with the temporarily assigned identity information is recycled or reused.

25. A data store residing in a computer-readable medium, for managing identity information, the data store comprising:

identity configuration information generated in response to a request made from a requestor for a service; and

temporarily assigned identity information generated for the identity configuration and used by the service for authenticating the requestor.

26. The data store of claim 25 further comprising a mapping that links the identity configuration with the temporarily assigned identity information, wherein the mapping is accessed for transmitting the temporarily assigned identity information along with the request to the service on behalf of the requestor.

27. The data store of claim 26 wherein the mapping is accessed for purposes of updating a protected identity directory that is accessed by the service in order to authenticate the request by using the temporarily assigned identity information.

28. The data store of claim 26 wherein the identity configuration, the temporarily assigned identity information, and the mapping are shared and managed

within the data store by a managing service and at least one additional service.

29. The data store of claim 26 wherein the mapping is cached and accessible for subsequent uses.

30. The data store of claim 26 wherein the mapping includes a collection of additional identity information which is not part of the identity information sent to the requestor.

31. The data store of claim 25 wherein the temporarily assigned identity information is a subset of identity information associated with the requestor.

32. The data store of claim 25 wherein the data store is a local identity mapping data store managed by a managing service and the data store is synchronized with another identity mapping store that is managed by another service.

33. The data store of claim 25 wherein the data store cannot be directly accessed by the service.

34. The data store of claim 25 wherein the data store is directly accessed by the service.